PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06, H04M 7/00 — A1

(11) International Publication Number: **WO 00/62507**

(43) International Publication Date: 19 October 2000 (19.10.00)

(21) International Application Number: PCT/US00/09323

(22) International Filing Date: 7 April 2000 (07.04.00)

(30) Priority Data:
60/128,772 9 April 1999 (09.04.99) US

(71) Applicant *(for all designated States except US)*: GENERAL INSTRUMENT CORPORATION [US/US]; 101 Tournament Drive, Horsham, PA 19044 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: MEDVINSKY, Sasha [US/US]; 8873 Hampe Court, San Diego, CA 92129 (US).

(74) Agents: TAGLIAFERRI, Daniel, D. et al.; Townsend and Townsend and Crew LLP, 8th floor, Two Embarcadero Center, San Francisco, CA 94111 (US).

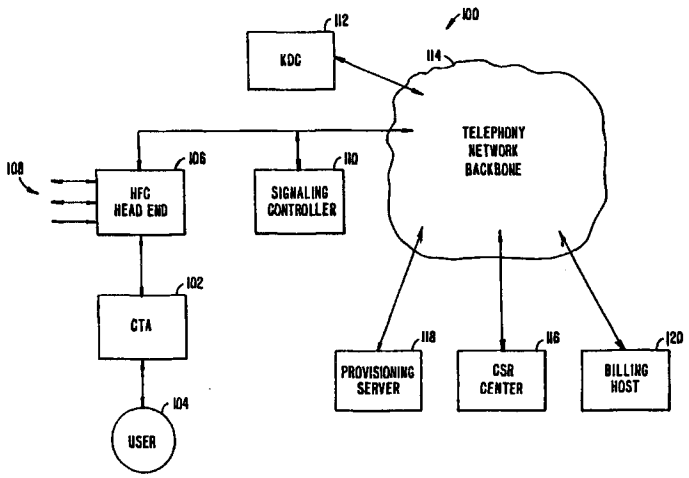
(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: KEY MANAGEMENT BETWEEN A CABLE TELEPHONY ADAPTER AND ASSOCIATED SIGNALING CONTROLLER



(57) Abstract

A highly scalable key management architecture for secure client–server systems used in IP telephony network, wherein cryptographic state needs to be saved only by the clients. This architecture takes advantage of existing key management protocols, Kerberos with the PKINIT (public key) extension, to provide an IP telephony system having a high degree of scalability. In the case of lost security associations, the architecture provides for lightweight rekeying operations that allow clients to quickly re–establish the lost association or switch to a different server. The key management architecture includes a method for establishing a secure channel between an IP telephony endpoint and Server in an IP telephony network. The endpoint is coupled to a user and the Server is coupled to the IP telephony network. The method comprises steps of transmitting from the endpoint to a key distribution center a request for a security ticket, receiving the security ticket from the key distribution center, transmitting from the endpoint to the Server a request for a sub–key, receiving the sub–key from the Server, and establishing a secure channel between the endpoint and the Server using the sub–key.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

KEY MANAGEMENT BETWEEN A CABLE TELEPHONY ADAPTER AND ASSOCIATED SIGNALING CONTROLLER

CROSS-REFERENCES TO RELATED APPLICATIONS

This application claims priority from co-pending U.S. Provisional Patent Application Serial No. 60/128,772 filed April 9, 1999, the disclosure of which is incorporated herein in its entirety for all purposes.

FIELD OF THE INVENTION

This invention relates generally to key management for Client-Server systems, and more particularly, to a scalable key management system for use in IP telephony networks.

BACKGROUND OF THE INVENTION

In an Internet Protocol (IP) telephony network, a network server may be responsible for setting up phone calls with up to 100,000 clients. The clients may be coupled to the telephony network via cable telephony adapter (CTA) devices. In order to secure call signaling, an Internet Protocol Security (IPSec) association is set up between each client and the server. This has to be done in a timely fashion to minimize the CPU overhead at the server and to minimize the call setup delay.

In order to handle large numbers of clients, key management needs to be as fast as possible. For example, security associations might be lost when a server goes down or become too busy to handle all of its clients. The lost security associations must then be re-establish again when needed. Manual administration of clients is unsuitable because of the high overhead costs and lack of scalability. Other techniques used in architectures unrelated to IP telephony are also not suitable, since they do not provide the desired scalability and low administration overhead.

SUMMARY OF THE INVENTION

The present invention includes a highly scalable key management architecture for secure client-server systems used in IP telephony network, wherein cryptographic state needs to be saved only by the clients. This architecture takes advantage of existing key management protocols, Kerberos with the PKINIT (public key) extension, to provide an IP telephony system having a high degree of scalability. In the case of lost security associations, the architecture provides for lightweight rekeying operations that allow clients to quickly re-establish the lost association or switch to a different server.

In one embodiment of the present invention, a method for establishing a secure channel between an IP telephony endpoint and Server in an IP telephony network is provided. The endpoint is coupled to a user and the Server is coupled to the IP telephony network. The method comprises steps of transmitting from the endpoint to a key distribution center a request for a security ticket, receiving the security ticket from the key distribution center, transmitting from the endpoint to the Server a request for a sub-key, receiving the sub-key from the Server, and establishing a secure channel between the endpoint and the Server using the sub-key.

A further understanding of the nature and the advantages of the inventions disclosed herein may be realized by reference to the remaining portions of the specification and the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows a telephony network constructed in accordance with the present invention;

FIG. 2 shows message exchange diagram for establishing a secure communication channel in accordance with the present invention; and

FIG. 3 shows a method for establishing a secure communication channel using the messages of FIG. 3.

DESCRIPTION OF THE SPECIFIC EMBODIMENTS

Embodiments of the present invention provide for establishing a secure channel between an IP telephony endpoint and a Server in an IP telephony network. In the embodiments discussed herein, a cable telephony adapter (CTA) device is

representative of the IP telephony endpoint and a Signaling Controller (SC) is representative of the Server. However, the present invention is suitable for use with other types of network endpoints and Servers not discussed herein.

FIG. 1 shows a portion of a telephony network 100 constructed in accordance with the present invention. To access the telephony network, CTA 102 provides access to a user 104 via a Hybrid Fiber/Coax (HFC) head-end 106. The HFC head-end 106 has the capacity to provide access to other users as shown at 108. The HFC head-end is also coupled to a Signaling Controller (SC) 110 which is coupled to a telephony network backbone 114. The Signaling Controller is used to control the CTA's access to the telephony network. A key distribution center (KDC) 112, is also coupled to the telephony network backbone 114. The KDC 112 issues Kerberos tickets, which are in turn used to generate sub-keys for secure connection protocols, such as the IPSec encapsulating security payload (ESP) protocol, or other secure connections. The network 100 also includes a customer service representative (CSR) center 116, a provisioning certification authority (CA) 118 and a billing host 120. Thus, in the network 100 it is possible for the user 104 to access the telephony backbone 114 via the CTA 102 using a secure protocol.

Embodiments of the present invention include the use of the Kerberos protocol with the public key PKINIT extension for key management. This protocol is based on Kerberos tickets, which are cookies, encrypted with the particular server's key. The Kerberos ticket is used to both authenticate a client to a server and to establish a session key, which is contained in the ticket. Accessing Kerberos services can be done using the Generic Security Service Application Program Interface (GSS-API) standard.

In one embodiment of the present invention, two-way authentication with public key certificates is used by the CTA to obtain a Signaling Controller ticket from the KDC. A corresponding session key is delivered to the CTA sealed with either the CTA's public key or with a secret derived from a Diffie-Hellman exchange. The Signaling Controller ticket is kept for a relatively long period of time, for example, days or weeks. The length of this period can be adjusted based on network performance requirements. In addition, the Signaling Controller ticket is used to establish a symmetric session key, which is in turn used to establish a set of keys for use with the IPSec ESP mode. The keys used by IPSec are not derived from the session key itself. Instead, another random key (i.e., a sub-key) is generated for each phone call and then used to derive the IPSec keys. Thus,

the Signaling Controller does not have to keep state. After it derives all the required keys from the sub-key and exchanges signaling messages with the CTA, the Signaling Controller can throw away the ticket along with all of the associated keys.

The use of the Kerberos protocol with the PKINIT extension in embodiments of the present invention provides several advantages. For example, the Signaling Controller is not required to keep state – Kerberos tickets need to be kept only by the endpoints (CTAs). Also, IPSec Security Associations can be torn down when no longer needed and quickly re-established with efficient key management based on the Kerberos tickets. The protocol runs over both TCP and UDP protocols, and is a widely available standard, with multiple vendors providing support for both Kerberos and PKINIT.

In one embodiment, within the PKINIT protocol, RSA is used for both key delivery and authentication. In another embodiment, a PKINIT option may be used wherein Diffie-Hellman is used for the key exchange and RSA is used for authentication. In general, embodiments of the present invention are suitable for use with any public key algorithms within PKINIT for both authentication and key exchanges.

FIG. 2 shows a message exchange diagram 200 illustrating how the CTA uses Kerberos to obtain the sub-key, which in turn, is used to derive IPSec ESP keys for the CTA-to-Signaling Controller signaling messages. In the exchange diagram 200, only some of the information carried in the messages is provided in order to present a clear description of the protocol. The exchange diagram 200 shows messages transmitted or received at the CTA 102 at line 220, the KDC 112 at line 222, and the Signaling Controller 110 at line 224.

FIG. 3 shows a flow diagram 300 illustrating how the messages of FIG. 2 are exchanged in accordance with the present invention.

At block 302, a PKINIT Request is sent from the CTA 102 to the KDC 112 as shown by message 202. This request includes the CTA signature and certificate - used by the KDC to authenticate the CTA. This request also carries the current time – used by the KDC to verify that this message is not a replay or a retransmission of an old message. The PKINIT Request also contains a random value (called a nonce) that will be used to bind a subsequent PKINIT Reply message to this request. In the case that a Diffie-Hellman exchange is used, the CTA will also include its Diffie-Hellman parameters and public value in the PKINIT Request.

At block 304, the KDC 112 receives and verifies the PKINIT Request and then issues to the CTA a ticket for the Signaling Controller encrypted with the Signaling Controller's service key. Inside this encrypted ticket are a symmetric session key, its validity period and the CTA identity. Also in this step, this ticket will be sent back to the CTA 102 inside a PKINIT Reply, shown by message 204. The PKINIT Reply message also contains KDC's certificate and signature for authenticating the KDC, along with the nonce from the PKINIT Request to protect against replays. If a Diffie-Hellman exchange is used, the KDC also places its Diffie-Hellman public value into this message.

The PKINIT Reply also contains a second copy of the session key and its validity period found in the ticket – intended to be decrypted and used by the CTA. This second copy of the session key and its associated attributes are either encrypted with a Diffie-Hellman-derived secret or enveloped with the CTA's public key. Here, enveloped means that the session key along with its associated attributes are not encrypted directly with the CTA's public key. Within the PKINIT Reply the public key is used to encrypt a random symmetric key that is in turn used to encrypt another symmetric key which is then finally used to encrypt the session key and its attributes. This embodiment uses the PKINIT standard as is, even though in this case, simplifications to the PKINIT Reply seem possible. If a Diffie-Hellman exchange is not used, then the Reply contains message items as shown at 226.

At block 306, an application (AP) Request is sent from the CTA 102 to the Signaling Controller 110 as shown by message 206. Here, a CTA has already obtained a Signaling Controller ticket and now initiates key management with the Signaling Controller by sending it an AP Request message. The AP Request contains the Signaling Controller ticket along with the CTA name, timestamp and a message hash – all encrypted with the SC session key. The timestamp is used to check for replays of old AP Request messages.

At block 308, the Signaling Controller 110 receives an AP Request. It first decrypts and validates the ticket with its service key. It then takes the session key out of the ticket and uses it to decrypt and validate the rest of the AP Request. Then, the Signaling Controller generates a random sub-key and encrypts it along with the current timestamp with the session key. It places this information into an AP Reply message 208 and sends it back to the CTA.

At block 310, the CTA receives and validates the AP Reply, after which it shares the sub-key with the Signaling Controller. Both sides independently derive (with some one-way function) a set of IPSec encryption and authentication keys from this sub-key. After that, all signaling messages between the CTA and the Signaling Controller will be protected with an IPSec channel. This establishment of the IPSec channel is symbolically illustrated in FIG. 2 at 210 – even though this step does not involve an exchange of messages.

In the embodiment of the invention depicted in FIGS. 2 and 3, the PKINIT exchange is performed at long intervals in order to obtain an intermediate symmetric session key. This session key is shared between the CTA and the Signaling Controller (via the Signaling Controller Ticket).

In this embodiment, the PKINIT Request/Reply messages, shown at 202 and 204, are sent over a TCP/IP connection. This is because a single PKINIT Request or Reply message, containing public key and Diffie-Hellman information may be too large to fit into a single UDP packet. The use of TCP instead of UDP may have some impact on performance, but since the PKINIT exchange occurs at infrequent intervals (days or weeks apart) and is not tied to the phone calls, the impact on performance is not significant.

The session key is used in the AP Request and AP Reply messages, shown at 206, 208 and are exchanged for each phone call, to establish a symmetric sub-key. This sub-key is used to derive all of the IPSec ESP keys and starting sequence numbers, used for both directions. The AP Request and AP Reply messages are small enough to fit into a single UDP packet, and thus will run over UDP.

The present invention provides a highly scalable key management architecture for secure client-server systems used in IP telephony networks. It will be apparent to those with skill in the art that modifications to the above methods and embodiments can occur without deviating from the scope of the present invention. Accordingly, the disclosures and descriptions herein are intended to be illustrative, but not limiting, of the scope of the invention which is set forth in the following claims.

WHAT IS CLAIMED IS:

1. A method for establishing a secure channel between an IP telephony endpoint and Server in an IP telephony network, wherein the endpoint is coupled to a user and the Server is coupled to the IP telephony network, the method comprising steps of:

transmitting from the endpoint to a key distribution center a request for a security ticket;

receiving the security ticket from the key distribution center;

transmitting from the endpoint to the Server a request for a sub-key;

receiving the sub-key from the Server; and

establishing a secure channel between the endpoint and the Server using the sub-key.

2. The method of claim 1, wherein the endpoint is a cable telephony adapter.

3. The method of claim 1, wherein the server is a Signaling Controller.

4. The method of claim 1, wherein the secure channel is an IPSec channel.

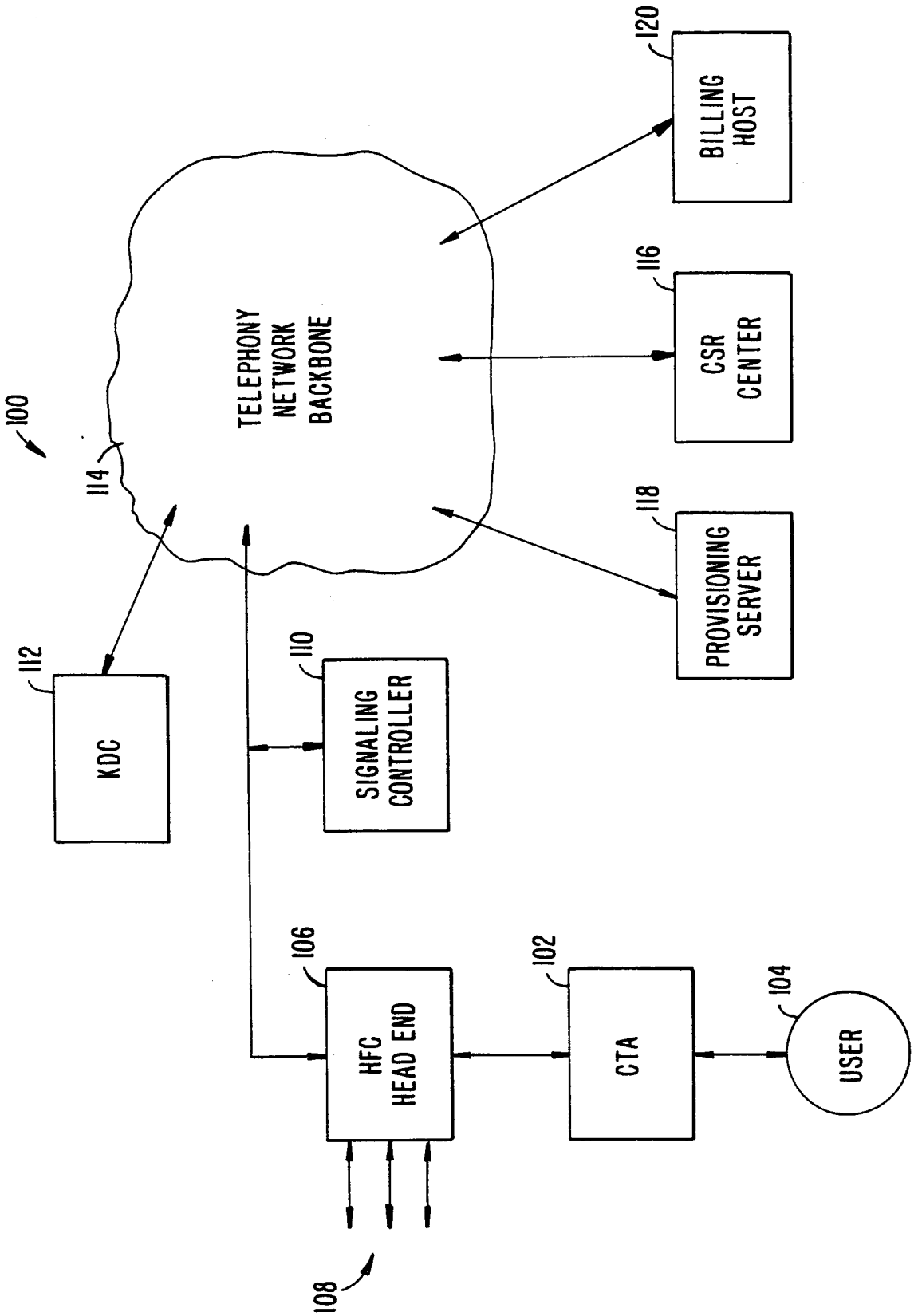

100
114
TELEPHONY NETWORK BACKBONE
120
BILLING HOST
116
CSR CENTER
118
PROVISIONING SERVER
112
KDC
110
SIGNALING CONTROLLER
106
HFC HEAD END
102
CTA
104
USER
108

FIG. 1.

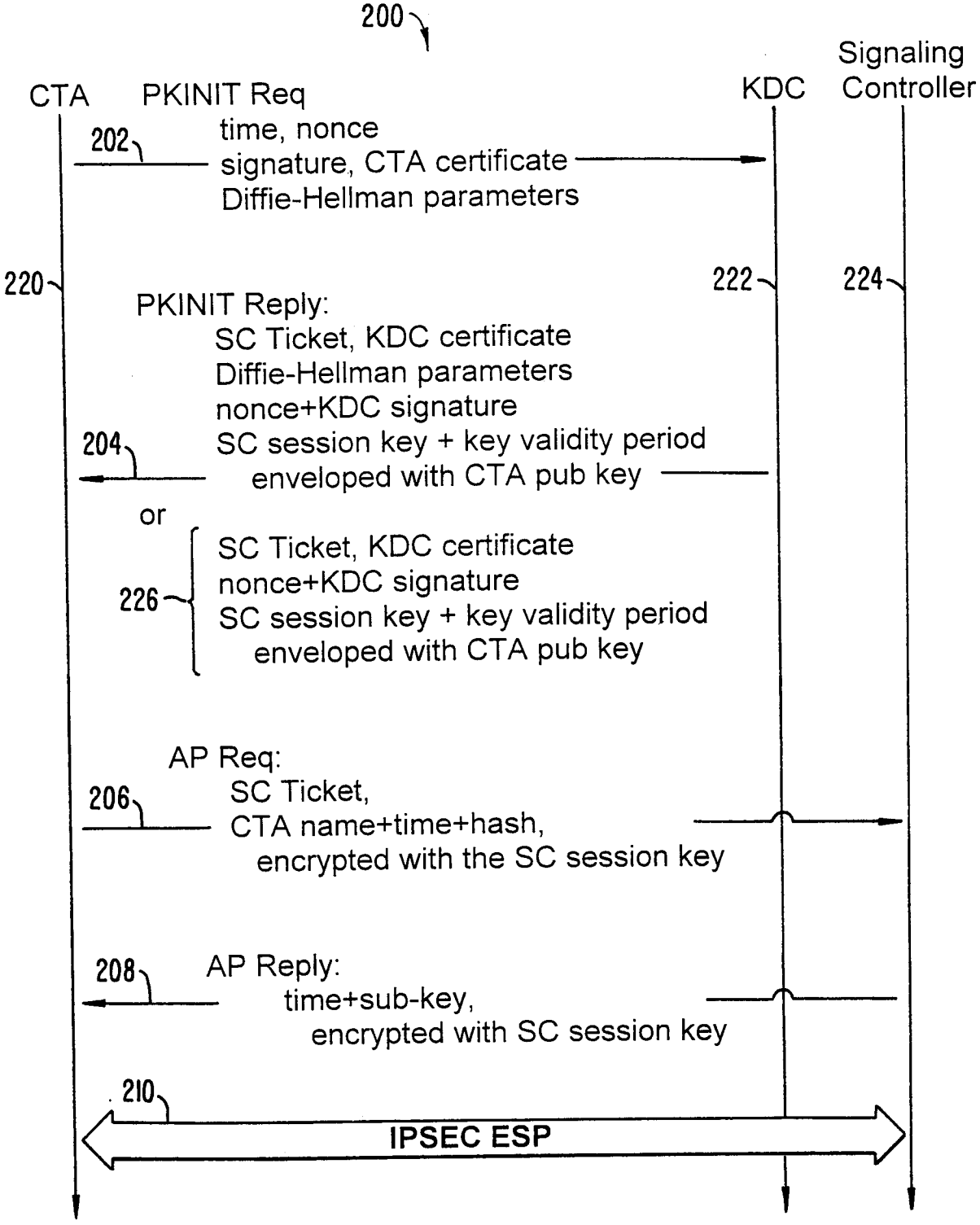

200
CTA
PKINIT Req
202
time, nonce
signature, CTA certificate
Diffie-Hellman parameters
KDC
Signaling Controller
220
222
224
PKINIT Reply:
SC Ticket, KDC certificate
Diffie-Hellman parameters
nonce+KDC signature
204
SC session key + key validity period
enveloped with CTA pub key
or
226
SC Ticket, KDC certificate
nonce+KDC signature
SC session key + key validity period
enveloped with CTA pub key
AP Req:
206
SC Ticket,
CTA name+time+hash,
encrypted with the SC session key
208
AP Reply:
time+sub-key,
encrypted with SC session key
210
IPSEC ESP

FIG. 2.

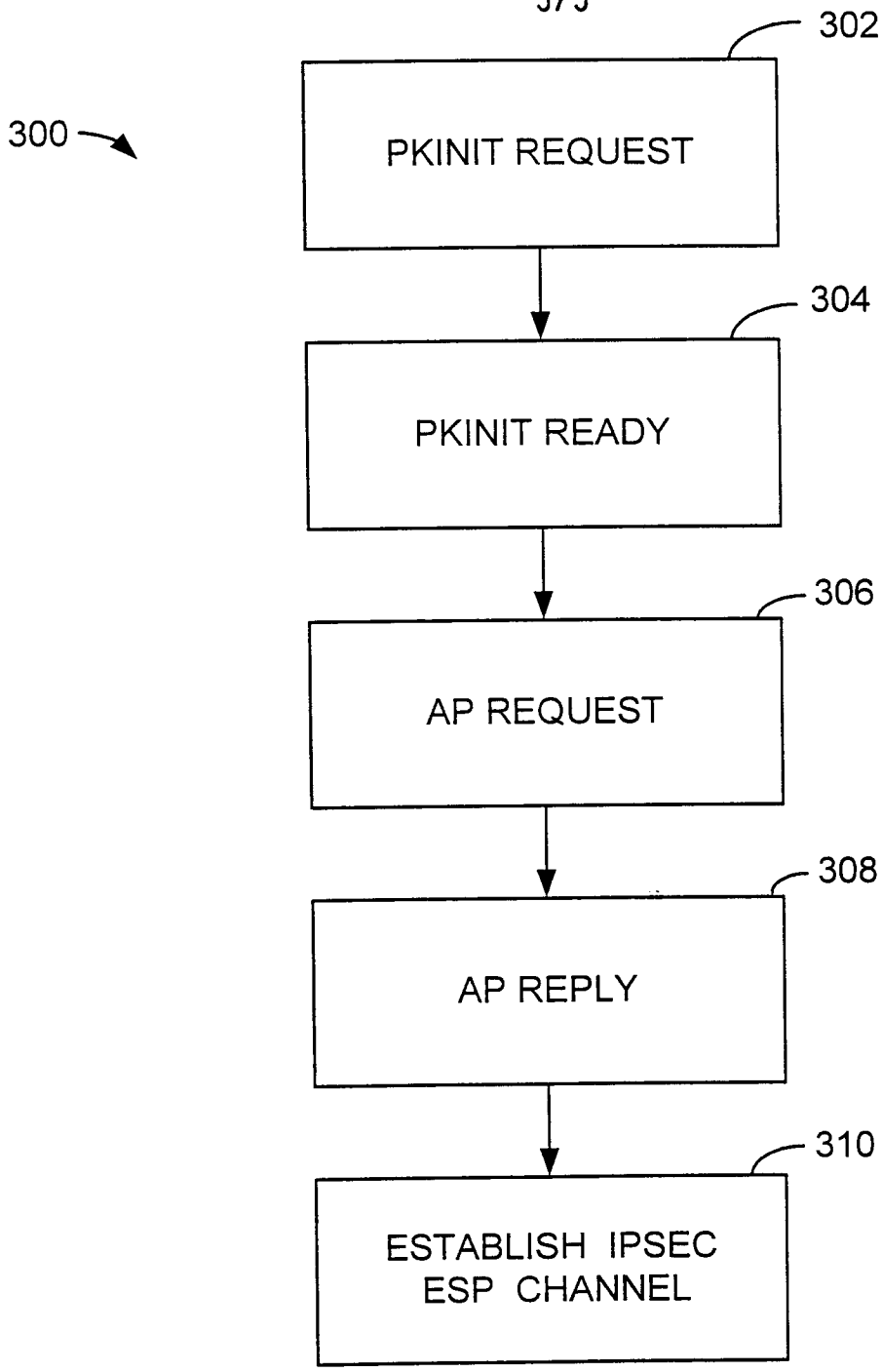

300
302
PKINIT REQUEST
304
PKINIT READY
306
AP REQUEST
308
AP REPLY
310
ESTABLISH IPSEC
ESP CHANNEL

FIG. 3.

INTERNATIONAL SEARCH REPORT

Int. .tional Application No
PCT/US 00/09323

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04M7/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and. where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 867 495 A (ELLIOTT ISAAC K ET AL) 2 February 1999 (1999-02-02) abstract column 77, line 31 -column 77, line 56 column 95, line 65 -column 96, line 23 column 133, line 7 -column 133, line 15 ---	1-4
A	WO 98 36522 A (GTE LABORATORIES INC) 20 August 1998 (1998-08-20) abstract page 8, line 7 -page 9, line 10 page 11, line 1 -page 14, line 12 figure 3 --- -/--	1-4

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 September 2000	28/09/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lai, C

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte .ional Application No
PCT/US 00/09323

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document. with indication,where appropriate. of the relevant passages	Relevant to claim No.
A	WO 97 47118 A (ERICSSON TELEFON AB L M ;HANSSON ALLAN (SE); TOENNBY INGMAR (SE)) 11 December 1997 (1997-12-11) abstract page 4, line 5 -page 4, line 15 page 5, line 10 -page 5, line 19 page 13, line 15 -page 13, line 35 page 14, line 21 -page 15, line 1 figure 1 ---	1-4
A	US 5 602 918 A (CHEN JAMES F ET AL) 11 February 1997 (1997-02-11) abstract column 2, line 42 -column 3, line 6 -----	1-4

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ..tional Application No
PCT/US 00/09323

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5867495	A	02-02-1999	AU	5686798 A	10-06-1998
			BR	9714315 A	08-02-2000
			EP	0950308 A	20-10-1999
			NO	992354 A	16-07-1999
			WO	9823080 A	28-05-1998
WO 9836522	A	20-08-1998	US	5923756 A	13-07-1999
			EP	0960500 A	01-12-1999
WO 9747118	A	11-12-1997	SE	506775 C	09-02-1998
			AU	3113697 A	05-01-1998
			AU	3113797 A	05-01-1998
			AU	3198597 A	05-01-1998
			AU	721188 B	22-06-2000
			AU	3198697 A	05-01-1998
			CN	1221530 A	30-06-1999
			CN	1221533 A	30-06-1999
			CN	1221531 A	30-06-1999
			CN	1221534 A	30-06-1999
			EP	0898837 A	03-03-1999
			EP	0898833 A	03-03-1999
			EP	0903031 A	24-03-1999
			EP	0898838 A	03-03-1999
			SE	9602212 A	05-12-1997
			SE	9603932 A	29-04-1998
			WO	9747127 A	11-12-1997
			WO	9746073 A	11-12-1997
			WO	9747119 A	11-12-1997
US 5602918	A	11-02-1997	CA	2241052 A	03-07-1997
			EP	0870382 A	14-10-1998
			JP	2000502532 T	29-02-2000
			WO	9723972 A	03-07-1997